Capgemini

Cloud Transformation DevOps Capability Service

G-Cloud 15

Table of Contents

1 Service Overview

Capgemini's Cloud DevOps transformation service provides an organisation with the ability to understand the current state of its cloud-based software delivery lifecycle and supports in defining the business case and roadmap for transformation, ultimately leading to increased software delivery performance.

Through value stream mapping of the existing software delivery lifecycle (SDLC), key metrics are identified related to delivery health. These include change lead time (how quickly a change can be delivered), process time (how long an activity takes), and the complete and accurate (correctness) ratio, which visualises any quality issues as a percentage of time spent on rework. The holistic approach of value stream mapping identifies and categorises waste in the wider process, helping uncover the most effective changes to improve overall efficiency. Our data-driven approach helps make a measurable impact.

The organisation's current ways of working are categorised using Capgemini's DevSecOps Framework, consisting of five key dimensions: Requirements Management, Engineering Practices, Process and Team Structure, Culture Management and Performance Management.

Requirements Management helps the organisation to understand and optimise the flow of feature requests to application and product developers, focusing on how to build the right things in the right way, utilising agile methodologies.

Engineering Practices identifies improvements that can positively impact the quality, reliability and speed of software delivery, achieved through detailed gap analysis using Capgemini's deep understanding of successful modern patterns and techniques.

The **Process and Team Structure** dimension helps organisations understand the optimal team structures and process and governance approaches that can reduce unnecessary bottlenecks and overheads that negatively affect the software delivery lifecycle.

Cultural Management focuses on the impact of the current culture and ways of working within and between the software development and operations teams on software delivery performance. We work with the organisation to adopt and embed DevSecOps best practices and ways of working that have been proven to act as force multipliers for engineering velocity.

Performance Management establishes a culture of measurable continuous improvement, ensuring organisations have the culture and skills to continue their journey beyond the end of their engagement with us.

In summary, Capgemini's Cloud DevOps transformation service helps organisations to become more agile, more efficient, and to deliver quicker in today's fast-paced digital landscape.

Note that while the name of our service calls out DevOps by name specifically, we strongly believe in the importance of integrating security into all phases of the software development lifecycle, and that organisations benefit greatly from addressing security as part of their overall transformation. To this end, we reference DevSecOps whenever we are referring to the practices of what we work with a company to embed.

2 Business Need

The business need for DevSecOps lies in its ability to enable organisations to deliver value to end users more quickly, efficiently, and reliably. Key reasons for adoption include:

1. Speed of delivery: A DevSecOps culture enables the acceleration of software delivery by streamlining development, testing, and deployment processes to reduce lead time and create and improve feedback loops. New features and subsequent improvements can be in the hands of end users faster than ever before.
2. Improved quality and reliability: Quality is critical for maintaining end-user satisfaction and trust. Continuous integration, continuous testing, and continuous delivery capabilities help deliver software with fewer defects and higher reliability. This leads to better customer experiences and reduces the risk of costly errors and downtime.

3. Increased efficiency and productivity: DevSecOps automates manual processes, eliminates bottlenecks, and reduces waste in the software delivery lifecycle. With the automation of repetitive tasks, organisations can improve efficiency, reduce manual effort, and optimise cloud resources. These help teams focus on value-added activities and deliver more with less.
4. Compliance: With standardisation and automation of practices, compliance checks can be tracked and recorded so that the software is compliant with regulations and organisations have end-to-end software development traceability.

3 Our Approach

Capgemini Cloud DevSecOps services can play a crucial role in helping businesses implement DevSecOps practices effectively.

Capgemini follows a four-phased approach in adopting DevSecOps aligned to organisation business objectives.

Phases 1 and 2: ***'DISCOVER' and 'INVESTIGATE'***

The Discover and Investigate phases are crucial stages in the transformation lifecycle and set the stage for a successful DevSecOps transformation that improves collaboration, efficiency, and agility across the organisation.

In the Discover phase, we work together with an organisation to assess its current state of culture, engineering practices, tooling, skills and business goals. This includes reviewing how code is developed, tested, deployed, and maintained, as well as how infrastructure is provisioned and managed.

The Investigate phase involves taking the outcomes of what we have learnt during the Discover phase and performing a gap analysis using our experience of what good looks like across these capabilities, i.e. our standard DevSecOps Framework.

Key aspects of these phases include:

Stakeholder analysis: We identify key stakeholders involved in the DevSecOps transformation, including developers, operations engineers, project managers, and executives. We understand their roles, responsibilities, and perspectives to ensure alignment and support for the DevSecOps initiative.

Inefficiency analysis: We identify gaps and areas of inefficiency in the current development and operations processes. This includes identifying bottlenecks, manual processes, silos between teams, and other barriers to collaboration and efficiency.

Business Objectives and Goals: We understand the organisation's strategic priorities and customer needs to align DevSecOps initiatives with broader business objectives.

Cultural Assessment: We assess the organisation's culture and readiness for DevSecOps adoption, including evaluating factors such as leadership support, organisation structure, communication patterns, and willingness to embrace change. We identify cultural barriers that may need to be addressed during the DevSecOps transformation.

Technology Stack Evaluation: We evaluate the organisation's technology stack, including development tools, infrastructure, and deployment pipelines. We assess the suitability of existing tools and technologies for supporting DevSecOps practices and identify any gaps or areas for improvement.

Skills and Training Needs: We assess the capabilities of the organisation's workforce in relation to DevSecOps practices, identifying training needs and skill gaps that need to be addressed so that teams have the necessary knowledge and expertise to implement DevSecOps effectively.

Tooling and Automation Opportunities: We identify opportunities for tooling and automation to improve development and operations processes. This includes evaluating tools for version control, continuous integration, continuous delivery, infrastructure as code, monitoring, and collaboration.

Metrics and Measurement: We define key performance indicators (KPIs) and metrics for measuring the success of the DevSecOps transformation. We identify metrics related to delivery speed, deployment frequency, lead time, change failure rate, and other factors that reflect the organisation's ability to deliver value to end users.

Phase 3: 'BLUEPRINT'

DevSecOps blueprinting refers to the process of creating a structured plan or framework for implementing DevSecOps practices within an organisation. It involves defining the key components, processes, and tools that will be used to support the DevSecOps transformation, based on the gap analysis performed in the Investigate phase. Put simply, where the Investigate phase details the 'what' is to be done, the Blueprint phase details the 'how'.

The steps involved in blueprinting include:

Roadmap and Implementation Plan: We develop a roadmap and implementation plan for adopting DevSecOps practices. We define specific initiatives, milestones, and timelines for implementing changes, addressing gaps, and achieving desired outcomes. We ensure that the roadmap is realistic, achievable, and aligned with business objectives.

Design of Processes and Workflows: We define the processes and workflows that will support the DevSecOps practices within the organisation. This involves mapping out how code will be developed, tested, deployed, and monitored throughout its lifecycle. We consider factors such as branching strategies, code review processes, release management, and incident response procedures.

Selection of Tools and Technologies: Together we choose the tools and technologies that will be used to support the DevSecOps practices defined in the blueprint. This may involve selecting tools for version control, CI/CD, infrastructure automation, monitoring, logging, collaboration, and other areas. Important factors Capgemini considers are ease of integration, scalability, and alignment with organisational requirements.

Integration and Toolchain Design: We design an integrated toolchain that connects the various DevSecOps tools and technologies. The toolchain will support end-to-end automation and visibility across the software delivery lifecycle, which involves configuring integrations between different tools, defining workflows, and setting up pipelines.

Definition of Roles and Responsibilities: We clearly define the roles and responsibilities of individuals and teams involved in the DevSecOps transformation. This includes roles such as developers, operations engineers, release managers, quality assurance testers, and security professionals. We ensure that everyone understands their roles and how they contribute to the overall DevSecOps initiative.

Creation of Cultural Guidelines: We develop cultural guidelines and best practices that support the adoption of DevSecOps principles within the organisation. This includes promoting collaboration, transparency, experimentation, and continuous learning, and encouraging a culture of shared ownership, accountability, and empowerment across teams.

Measurement and Feedback Mechanisms: We define key performance indicators (KPIs) and metrics for measuring the success of the DevSecOps transformation. We establish mechanisms for collecting, analysing, and acting on feedback from stakeholders, users, and monitoring systems. We use metrics to track progress, identify areas for improvement, and drive continuous optimization.

Training and Education: We provide training and education to teams through our Cloud Academy to ensure that they have the knowledge and skills needed to adopt and implement DevSecOps practices effectively. We offer workshops, courses, and resources to help teams learn about DevSecOps concepts, tools, and best practices.

Continuous Improvement and Iteration: We recognise that blueprinting is an iterative process and that the blueprint will evolve over time. We encourage teams to experiment, learn from failures, and continuously improve their processes and practices. Capgemini enables fostering a culture of continuous improvement and adaptation to help ensure that the transformation remains effective and relevant.

By following these steps, organisations can create a blueprint that provides a clear roadmap for implementing DevSecOps practices and achieving the desired business outcomes. The Capgemini DevSecOps blueprint serves as a guide for teams to follow as they embark on their DevSecOps journey.

Phase 4: 'IMPLEMENT'

The Implement phase is where the recommendations from the Blueprint phase are delivered. Typical activities in this phase include:

Platform Selection: We help and advise on choosing a robust DevSecOps platform that provides a comprehensive set of tools and capabilities for integrating security into the pipeline. This platform should support automation, collaboration, and scalability to meet the needs of your organisation.

Automated Security Scanning: We integrate automated security scanning tools into the pipeline to scan code, dependencies, containers, and infrastructure for vulnerabilities. These tools perform static code analysis, dynamic application security testing (DAST), software composition analysis (SCA), container security scanning, and infrastructure security checks.

Continuous Monitoring and Compliance: We help implement continuous monitoring and compliance checks so that security requirements are met throughout the software development lifecycle. We utilize tools for logging, monitoring, and auditing to track changes, detect anomalies, and enforce security policies.

AI-driven Threat Detection: We leverage generative AI algorithms to analyse security data, identify patterns, and detect potential threats and vulnerabilities. AI-powered threat detection can help automate the process of identifying and prioritizing security issues, enabling teams to respond more quickly and effectively.

Automated Remediation: We implement automated remediation workflows to address security issues identified during the pipeline. This may involve automatically applying patches, updating dependencies, or reconfiguring infrastructure to mitigate vulnerabilities. We assist with the adoption of AI-driven decision-making to prioritize and execute remediation actions based on risk levels and impact.

Policy Enforcement and Governance: We enforce security policies and governance requirements throughout the pipeline to comply with regulatory standards and industry best practices. We make use of AI-powered analytics to assess policy adherence, identify compliance gaps, and enforce security controls proactively.

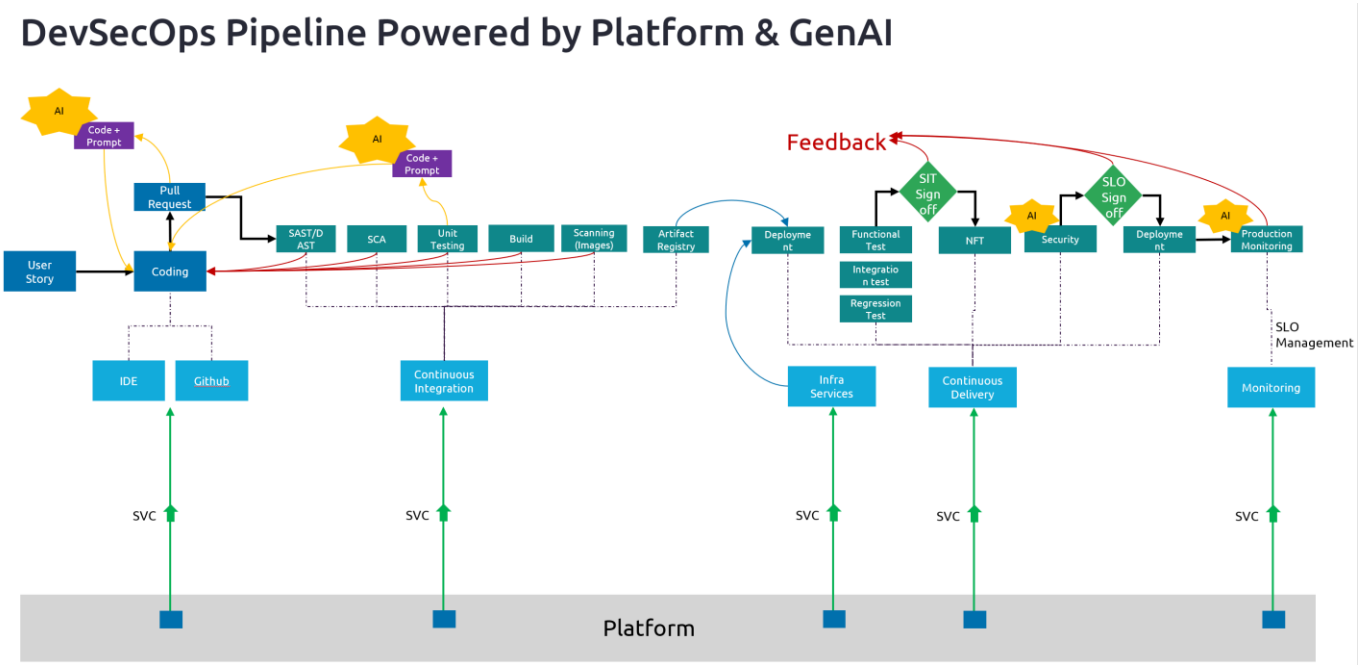
Collaborative Security Culture: We foster a collaborative security culture by integrating security into the development process and promoting cross-functional collaboration between development, security, and operations teams. We use AI-driven insights to facilitate communication, knowledge sharing, and alignment on security priorities.

Continuous Improvement and Optimization: We continuously monitor and analyse pipeline performance to identify opportunities for optimization and improvement. Using AI algorithms we analyse metrics, identify bottlenecks, and recommend optimizations to streamline the pipeline and enhance security posture.

Feedback Loops and Learning: We establish feedback loops to capture insights and lessons learned from security incidents, breaches, and near misses. AI-driven analytics are used to analyse incident data, identify root causes, and derive actionable insights for improving security practices and mitigating future risks.

Adaptive Security Controls: We implement adaptive security controls that can dynamically adjust based on changing threats, vulnerabilities, and environmental conditions. We make use of AI-driven decision-making to adapt security policies, configurations, and controls in real-time to mitigate emerging risks and protect against evolving threats.

The visual below illustrates how a number of these capabilities come together through the creation of a DevSecOps pipeline, showing the journey of a feature from user story through implementation, build and testing, all the way to production and post-production monitoring. By building a DevSecOps pipeline powered by a platform and leveraging generative AI, Capgemini enables organisations to automate security practices, improve threat detection and response, and enhance overall security posture while accelerating software delivery and innovation. This approach enables organisations to achieve the dual goals of security and agility.



A DevSecOps pipeline powered by Platform & Gen AI.

4 Buyer Responsibilities

Please refer to the Supplier Terms listed with this service on the Platform. These may contain additional Buyer obligations/costs the Buyer is subject to that are not identified anywhere else in the Supplier's Application or on the Platform.

The Buyer responsibilities as part of this service are as follows:

- Provide reasonably requested resources, stakeholders, information, and materials in a timely manner.
- Provide access to the appropriate process and subject matter experts to work with Capgemini to agree the design of the solution.
- Ensure that business users are available to perform user acceptance testing based on the agreed plan.
- Procure the necessary software licenses and subscriptions as appropriate.
- Provide access to existing systems or the data from the existing systems to enable data migration.
- Provide test instances of any 3rd party systems that will be required to test inbound or outbound interfaces.
- Ensure employees are made available for training as appropriate.
- Ensure the Buyer's project team is empowered to make the decisions necessary in a quick and timely manner.
- Review and sign-off all deliverables in a timely manner based on agreed acceptance criteria.

If these responsibilities do not match your expectations, then please contact us in order that we can explore options to vary our approach.

5 Service Management

This service can be delivered as a defined project or on a day rate basis. In either case it will be a clearly defined project with agreed processes, outputs, and deliverables.

Capgemini will establish the required multi-level project governance and delivery assurance including regular reporting at the beginning of the project.

6 Protection of Data

This service is based on a security classification of 'Official', however should you have a requirement for a different security classification that you would like us to consider, please contact us to discuss.

7 On-boarding and Off-boarding

Prior to the execution of the Order, the Supplier and the Buyer will agree the scope of the exit plan for the Services and a timescale for delivering an exit plan to ensure continuity of service.

Capgemini shall undertake on-boarding and off-boarding activities agreed within the Order Form and an exit plan in line with the Call-Off Contract terms which will be charged for in accordance with the Pricing section for this service.

8 Skills and Knowledge Transfer

Capgemini recognises that skills and knowledge transfer is a critical element in the provision of G-Cloud services to public sector clients. Where possible and applicable, this forms part of the delivery plan for the service agreed at the start of the engagement. Our consultants and engineers are experienced in providing skills and knowledge transfer for major private and public sector clients.

Where appropriate, we may use a standard approach, tailored to topic, skills-gap and individual, to ensure consistency and effectiveness. The approach, Capgemini's Assess-Plan-Implement framework, has been used repeatedly by our teams to structure the work involved in transferring skills and creating new teams capable of driving and sustaining change long after the end of the formal programme. The framework can be applied throughout a project to understand knowledge transfer objectives, plan training delivery methods and materials, and deliver and evaluate success.

9 Vendor Accreditations/Awards

For the 13th year in a row, Capgemini has been recognised as one of the World's Most Ethical Companies® by the Ethisphere® Institute. This is an acknowledgement of our ethical culture that makes us an employer of choice and responsible player in the eyes of our clients, shareholders, and the wider community.

ISO 9001 Quality Management for Management Consultancy and IT Implementation and services to the Public Sector

ISO 27001:2013 - Provision (Delivery) of IT services including business applications development, maintenance and Data, Digital and Cloud technologies.

NelsonHall has identified Capgemini as a Leader in its 2022 NEAT Vendor Evaluation for Learning Services due to its ability to meet future client requirements as well as its capability to deliver immediate learning benefits to them.

Capgemini is the first amongst consultancy and technology firms to be recognized six times in a row for its thought leadership reports.

2023 Ecovadis Platinum Rating: We maintained a platinum rating, recognising us as a responsible and sustainable business in the top 1% of companies assessed.

Better Society Awards: Our collaboration with Code Your Future to offer digital skills training won a Better Society Award in 2022. The awards celebrate efforts by commercial organisations to create a better society.

Inclusive Top 50 UK Employers List: We achieved second place in the Inclusive Top 50 UK Employers List 2022/23 – a list that assesses companies for best practice on diversity, equality and inclusion

UK Best Workplaces for Women: We were listed as a Best Workplace for Women by Great Place to Work®. This listing is based on responses from our team to an anonymous survey about their employee experience.

UK Best Workplaces for Wellbeing : We are listed by Great Place to Work® as a Best Workplace for Wellbeing

Great Place to Work: We were certified as a Great Place to Work® in 2023, reflecting our employees' experience of working at Capgemini in the UK.

10 Sub-contractors

Capgemini UK may use the following subcontractors to deliver this service:

- Capgemini Technology Services India Limited.

11 Business Continuity and Disaster Recovery

Disaster recovery solution may be included in the target solution if it part of the customer's requirement.

12 Pricing

This service is priced in accordance with the SFIA Rate Card attached. Capgemini can also provide offshore resources at reduced rates where appropriate. Projects can be priced either on a Time & Materials or Fixed Price basis.

All prices are in GBP and exclude VAT.

13 Ordering and Invoicing

Please refer to the Supplier Terms for this service.

We would be pleased to arrange a call or meeting to discuss your requirements of our service in more detail.

14 Termination Terms

Please refer to the Supplier Terms for this service.

15 Further Information

For more information about this or any of our G-Cloud services, please contact our Public Sector Team.

Phone: 0370 904 4858

Email: publicsector.opps.uk@capgemini.com including the following information:

1. The name of this service.
2. The name of your organisation.
3. Your name and contact details.
4. A brief description of your business situation.
5. Your preferred timescales for starting the work.

About Capgemini

Capgemini is a global business and technology transformation partner, helping organizations to accelerate their dual transition to a digital and sustainable world, while creating tangible impact for enterprises and society. It is a responsible and diverse group of 340,000 team members in more than 50 countries. With its strong over 55-year heritage, Capgemini is trusted by its clients to unlock the value of technology to address the entire breadth of their business needs. It delivers end-to-end services and solutions leveraging strengths from strategy and design to engineering, all fueled by its market leading capabilities in AI, generative AI, cloud and data, combined with its deep industry expertise and partner ecosystem. The Group reported 2024 global revenues of €22.1 billion.

Make it real. | www.capgemini.com